

REMARKS

Applicants respectfully request reexamination of the above-identified patent application. Claims 1-16 are pending in the present application. Claims 1 and 2 have been amended for purposes of clarification.

In an Office Action of November 13, 2007 (hereinafter "Office Action"), Claims 1-16 were rejected under 35 U.S.C. § 102(b) as being anticipated by White et al., "Anatomy of a Commercial-Grade Immune System," <<http://citeseer.ist.psu.edu/white99anatomy.html>> 1999 (hereinafter, "White"). Applicants respectfully disagree. Even though applicants disagree, in the interest of advancing prosecution of the present application, applicants have made minor amendments to Claims 1 and 2. These minor amendments do not change the scope of the claims and have been made only to clarify the claim language.

Pursuant to 37 C.F.R. § 1.111 and for the reasons set forth below, applicants respectfully request reconsideration and allowance of the pending claims. Prior to discussing the reasons why applicants believe that all of the claims of the present application are allowable over the cited reference of White, and hence in condition for allowance, brief summaries of the claimed subject matter and White are presented. However, while the brief summaries are presented to assist the Examiner to appreciate the differences between the claimed subject matter and White, they should not be viewed as limiting upon the disclosed subject matter.

Summary of the Claimed Subject Matter

In order to better appreciate the differences between the claimed subject matter and other anti-virus systems, including White, most anti-virus software recognizes viruses according to a "signature" computed/derived from the malware itself. In a general sense, when a suspected file arrives, a hash or checksum (which yields fairly unique results over a corpus body of files) is generated of that suspected file. The resulting hash or checksum value is then compared to hash

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206 682 8100

or checksum values of known malware, and if there is match, the suspected file is therefore identified as malware. The problem with this type of identification is twofold: (1) for a hash or checksum to generate relatively unique results over a corpus body of files, small modifications to a file will result in a different hash or checksum value; and (2) malware exploits this by being self-polymorphic, i.e., it has the ability to modify itself without changing its underlying function to the end that it cannot be recognized according to a hash or checksum value/signature based on the file itself. The claimed subject matter addresses these issues.

The claimed subject matter is generally directed to determining whether a code module represents malware (i.e., a virus, worm, Trojan horse, etc.) according to behaviors of the code—the underlying behaviors—and not a hash or checksum value of the code. In this way, polymorphic malware cannot simply change its outward appearance and escape detection.

According to the claimed subject matter, when a code module is received, a behavior evaluation module is selected that corresponds to the particular code module. The code module is then executed within the selected behavior evaluation module. Executing the code module exposes the underlying behavior of the malware. As the code module is executing, some of the behaviors/actions that the code module makes are recorded. The recorded behaviors of the code module are then compared to recorded behaviors of known malware to determine whether there is a match, i.e., that the code module is known malware.

Additional aspects of the claimed subject matter include, for each behavior evaluation module, a predefined set of behaviors to record if/when they occur. Moreover, in one embodiment, the predefined set of behaviors corresponds to a predefined set of system calls that are viewed as "interesting," i.e., a behavior (system call) worthy of recording in a behavior signature.

In sum, the claimed subject matter is directed to identifying malware according to its underlying functionality, i.e., according to its exhibited behaviors. No other system identifies malware according to its underlying functionality. Instead, other systems identify a suspected file as malware according to a signature derived from the suspected file.

Summary of White

White purportedly describes a system for discovering new viruses, creating a "cure" for the new virus, as well as a signature for future identification. However, in the process of discovering new viruses, White explicitly describes that it first tries to identify a file as malware (or as a clean file) according to a checksum of the file. More particular, the file (hereinafter "file A") is submitted to an Administrator system that generates a checksum (signature) of file A and compares that value to values of files known to be clean and files known to be malware. White, page 14. If file A cannot be determined to be a clean file or malware, it is forwarded to a gateway where the latest virus definitions are found, and the signature is again checked for malware or clean file. Only when file A has not been previously identified is file A delivered to an analysis center. As generally explained above with respect to the claimed subject matter, a malware and a modified version of the malware will have different checksums, yet have the same underlying functionality. Accordingly, White is never able to recognize from the different checksums of a file and its modified version that the underlying functionality of file A and a modified file A, for example, are essentially the same.

At the analysis center, file A is classified. Classification permits White to apply specialized type-specific routines to analyze the underlying behavior of file A. After file A is classified, replications of file A (samples of file A) are executed on different virtual systems so that a sufficient analysis of the results of the infection of file A can be determined, as found in "goat" files. White, page 21. Analysis is performed and a set of source files are produced from

which a definition file for file A is generated. The definition file generated contains full verification information. Finally, the generated definition file is tested to properly detect, verify, and disinfect all samples of file A. Only when the definition file can properly detect, verify, and disinfect all samples of file A without any exceptions is the definition file submitted as a solution to detect, verify, and disinfect future files classified similar to file A. Nothing in White teaches recording some of the behaviors during execution of the different samples of file A and comparing the recorded behaviors of file A against recorded behaviors of files previously classified similar to file A and known to be malware to identify/determine file A as malware.

The Claims Distinguished: 35 U.S.C. § 102(b) Rejections

Claim 1

The Office Action asserts that White discloses each and every element of Claim 1.

Applicants respectfully disagree. Applicants submit that White fails to disclose:

a behavior signature comparison module that obtains the behavior signature of the code module and compares the behavior signature of the code module to the known malware behavior signatures in the malware behavior signature store to determine whether the exhibited execution behaviors of the code module match the exhibited execution behaviors of a known malware.

The Office Action (page 2) asserts that White discloses that virus samples are stored at page 2, paragraph 7. Applicants fail to find the aforementioned assertion anywhere in White, let alone at page 2, paragraph 7. The Office Action (page 2) further asserts that White discloses that a comparison is made between the archived samples and the virus definition to determine exact matches at page 23, paragraph 1. Applicants respectfully disagree. White uses "matches" at page 23, paragraph 1, as a noun and not as a transitive verb. Nowhere does White explicitly or implicitly teach "compares," i.e., "to examine the character or qualities of especially in order to discover resemblances or differences," as recited in Claim 1. What White is referring to on page

23, paragraph 1, is the disinfection of a future file using a known virus definition file only if the future file, during the analysis phase discussed above (see Summary of White), generates a definition file identical to a known virus definition file. If White makes any comparison, it is between a known virus definition file and a definition file generated during the analysis of a future file. Nowhere does White explicitly or implicitly teach comparing a behavior signature of a future file with a known malware behavior signature.

The Office Action (page 4) asserts that White at pages 13-15, paragraph 5, lines 1-2, teaches a gateway that scans the sample file against the latest virus definition to read on a behavior signature comparison module that obtains the behavior signature of the code module, and compares the behavior signature of the code module to the known malware behavior signatures in the malware behavior signature store to determine whether the exhibited execution behaviors of the code module match the exhibited execution behaviors of a known malware. Applicants respectfully disagree. Paragraphs 4 and 5 at pages 14 and 15 clearly disclose a gateway to have two primary functions. The gateway's first function is to see if it can handle the sample without forwarding the sample to a higher node in the active network. The gateway accomplishes this by matching a checksum of the sample file with a database of checksums. As noted above with respect to the claimed subject matter (see Summary of Claimed Subject Matter), a malware and a modified version of the malware will have different checksums, yet have the same underlying functionality. Since matching checksums is not the same as comparing the behavior signature of the sample to the known malware behavior signatures in the malware behavior signature store to determine whether the exhibited execution behaviors of the sample match the exhibited execution behaviors of a known malware, White fails to teach "...compares the behavior signature of the code module to the known malware behavior

signatures in the malware behavior signature store to determine whether the exhibited execution behaviors of the code module match the exhibited execution behaviors of a known malware."

The gateway's second function is to scan the sample with the latest virus definition files. Since scanning the sample with the latest definition files is not the same as comparing exhibited execution behaviors of the sample with the exhibited execution behaviors of files classified in the same category as the sample, White again fails to teach ". . . compares the behavior signature of the code module to the known malware behavior signatures in the malware behavior signature store to determine whether the exhibited execution behaviors of the code module match the exhibited execution behaviors of a known malware."

As explained above, White fails to teach or suggest a malware detection system for determining whether a code module is malware according to the code module's exhibited behavior comprising a behavior signature comparison module that obtains the behavior signature of the code module and compares the behavior signature of the code module to the known malware behavior signatures in the malware behavior signature store to determine whether the exhibited execution behaviors of the code module match the exhibited execution behaviors of a known malware. In light of the amendments to Claim 1 and in view of the remarks above, applicants submit that White fails to disclose each and every element of Claim 1. Accordingly, applicants respectfully request withdrawal of the pending rejection under 35 U.S.C. § 102(b) with regard to Claim 1, and the allowance of Claim 1.

Claim 2

Applicants point out that, while differing in scope, independent Claim 2 recites substantially similar elements to those found in independent Claim 1, including elements not found in White. In particular, Claim 2 recites:

a behavior comparison means for comparing the behavior signature of the code module to the known malware behavior signatures in the storage

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PLLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206 682 8100

means to determine whether the exhibited execution behaviors of the code module match the exhibited execution behaviors of a known malware.

In this light, applicants submit that the arguments set forth with regard to Claim 1 are equally applicable with regard to Claim 2. Accordingly, applicants respectfully request withdrawal of the pending rejection under 35 U.S.C. § 102(b) with regard to Claim 2, and the allowance of Claim 2.

Claims 3 and 4

Applicants point out that, while differing in scope, independent Claims 3 and 4 recite similar elements to those found in independent Claim 1, including elements not found in White. In particular, Claims 3 and 4 include the following:

comparing the recorded execution behaviors exhibited by the code module executing in the dynamic behavior evaluation module to known malware execution behaviors.

In this light, applicants submit that the arguments set forth with regard to Claim 1 are equally applicable with regard to independent Claims 3 and 4. Accordingly, applicants respectfully request withdrawal of the pending rejection under 35 U.S.C. § 102(b) with regard to Claims 3 and 4, and the allowance of Claims 3 and 4.

Claims 5-16

Claims 5-7 depend from independent Claim 1, Claims 8-10 depend from independent Claim 2, Claims 11-13 depend from independent Claim 3, and Claims 14-16 depend from independent Claim 4. As discussed above, White fails to teach each and every element of independent Claims 1-4. Accordingly, for the above-mentioned reasons, Claims 5-16 are also not anticipated by White. Accordingly, applicants respectfully request withdrawal of the pending rejection under 35 U.S.C. § 102(b) with regard to Claims 5-16, and the allowance of Claims 5-16.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PLLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206 682 8100

CONCLUSION

In view of the above amendments and remarks, applicants respectfully submit that the present application is in condition for allowance. Reconsideration and reexamination of the application and allowance of the claims at an early date are solicited. If the Examiner has any questions or comments concerning the foregoing response, the Examiner is invited to contact the applicants' undersigned attorney at the number provided below.

Respectfully submitted,

CHRISTENSEN O'CONNOR
JOHNSON KINDNESS^{PLLC}

A handwritten signature in black ink, appearing to read "Clint J. Feekes", is written over the printed name. To the right of the signature, the number "53479" is handwritten.

Clint J. Feekes
Registration No. 51,670
Direct Dial No. 206.695.1633

CJF:jljg

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PLLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206 682 8100